UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/390,363	09/07/1999	JON N. LEONARD	BEU/LEONARD	6725

7590   02/24/2004

BACON & THOMAS
625 SLATERS LANE 4TH FLOOR
ALEXANDRIA, VA 223141176

EXAMINER
DADA, BEEMNET W

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 02/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _05 December 2003_.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-50_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-50_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2.   Claims 18-32 are rejected under 35 U.S.C. 102(e) as being anticipated by

Anderson (U.S. Patent No. 6,442,600 B1).

3.   As per claim 18, Anderson teaches a method of controlling an electronic mail

message transmitted over a network, comprising the steps of:

        before transmission of the electronic mail message over the network, attaching to

the message a date, time, or event, the occurrence of which will cause said electronic

mail message and all designated incarnations thereof to expire (column 3, lines 62-67);

and

encrypting said electronic mail message so that it can only be viewed before the

occurrence of said time, date or event using viewer applet installed on recipient

computer (column 5, lines 25-30, and column 4, lines30-34).

4.   As per claims 19, 20, 24, and 25, Anderson discloses a method of controlling an

electronic mail message transmitted over a network (i.e. system for distributing

electronic messages, see figure 1) further comprising a central electronic mail server

(i.e. Message Distribution server (MDS), see figure 1) connected to the network 140.

Anderson discloses the message sender to supply the electronic message to the MDS

and the MDS will stores the message and is responsible for forwarding it to the recipient

[see column 5 lines 19-50]. Anderson also discloses the MDS will retrieve the public key

from the recipient and encrypt the electronic message upon request by the recipient and

stream it to corresponding recipient [see figure 6 steps 625,630,635,640]. The recipient

can access the message by decrypting it using the private key of the recipient computer

system's private key and display said electronic message [see column 6 lines 16-29].

5.   As per claim 21, Anderson discloses the recipient (i.e. a user) can select a

message and indicate a message forwarding action to be taken (i.e. forward to a

second recipient computer, see figure 2 and column 6 lines 46-65). Anderson discloses

the message distributor subroutine of MDS (i.e. central mail server) being arrange to

encrypt the message using the public encryption key generated in the recipient

computer s, stem [see column 5 lines 58-63] and send it to each Y recipient [column 9 lines 9-16].

6.   As per claims 22 and 23, Anderson discloses the central electronic mail server (i.e. MDS) erases (i.e. deletes) the single copy of the electronic message when the end of a maximum time period has expired [see column 4 lines 25-44].

7.   As per claims 26-28, Anderson discloses the electronic message (i.e. E-mail) is encrypted in the central mail server (i.e. Message Distribution Server) with the recipient's public key before transmission to said recipient computer [see column 10 lines 5-14 and figure 6 steps 625,630,635,640].

8.   As per claim 29, Anderson discloses Message Receiver (MR) stores the decrypted message indicator (i.e. e-mail) in an encrypted fashion on the recipient computer system [see column 6 lines 16-29] and erase (i.e. delete) the message if the expiration period has ended (i.e. upon the occurrence of said date, time, or event, see column 9 lies 64-66).

9.   As per claim 30-31, Anderson discloses the recipient (i.e. a user) can select a message and indicate a message forwarding action to be taken (i.e. forward to a second recipient computer, see figure 2 and column 6 lines 46-65). Anderson discloses the message distributor subroutine of MDS (i.e. central mail server) being arrange to

encrypt the message using the public encryption key generated in the recipient

computer system [see column 5 lines 58-63] and send it to each recipient [column 9

lines 9-16].

10.   As per claim 32, Anderson discloses the message origination software (i.e.

message sender 154, see figure 1) arranged to permit the message to include the

expiration time (i.e. limitation, see column 3 lines 62-65) before transmission over said

network 140 [see column 3 lines 48-66 and figure 2).

Claim Rejections - 35 USC § 103

11.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

12.   Claims 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Anderson as applied to claims 18 and 32 above.

13.   As per claim 33, Anderson does not expressly disclose the processing and

handling limitations are implemented by said view applet (i.e. the message receiver

155). It would have been obvious to a person of ordinary skill in the art at the time of

invention was made to implement the request from the message receiver 155 (i.e. view

applet) of the message recipient to review, save, or delete an indicated message (i.e.

processing and handling limitations) with in the system of Anderson because it's well

known in the art to activate the subroutine software such as view applet in the recipient

computer system to handling the access limitation of the electronic message.

14.   Claims 1-17, and 34-50 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Anderson (U.S. Patent No. 6,442,600 B1) in view of Udell et al

(hereinafter refereed to as Udell) (U.S. Publication No. 2003/0126215 A1).

15.   As per claim 1, Anderson discloses an electronic mail system (i.e. system for

distributing electronic messages, see figure 1) comprising:

        a) a first computer 150 (i.e. the sender, see column 3 lines 61-63) which is

connect to a network 140 capable of carrying an electronic mail message (i.e.

transmission of the electronic messages, see column 4 line 65- column 5 line 1);

        b) recipient computers systems (elements 160, 170, and 180; see figure 1) are

connected to network 140 [see column 4 lines 59-65];

        c) a view applet (i.e. the message receiver 155 with the URL, the web browser

software, see column 4 lines 13-16);

        Anderson discloses the electronic message (i.e. e-mail) includes minimum or

maximum expiration time periods (i.e. time is attached to the electronic mail message

prior to transmission over network, see column 3 lines 62-67) will cause the electronic

message and all designated incarnations thereof to expire. Anderson also discloses the

electronic message (i.e. e-mail) is encrypted so that it may only be viewed using said

view applet (i.e. URL web browser) upon installation of said view applet on the recipient

computers (i.e. element 160, 170, 180, see figure I and column 5 lines 25-30).

Furthermore, Anderson teaches deleting encrypted message when time period

that is associated with the message has expired [column 4, lines 30-35, column 5, lines

24-26]. Anderson also teaches providing recipient access restrictions [column 4, lines 3-

7]. Anderson does not explicitly teach preventing decryption and viewing of encrypted

messages by a recipient after the occurrence of date, time or event selected by the

originator of the message.

However, Udell teaches a viewer applet (i.e. application program (Microsoft

outlook), see page 6, paragraph 0064) is arranged to prevent decryption and viewing of

encrypted electronic mail message by a recipient after the occurrence of the date, time

or event by said originator of the electronic mail message (page 2, paragraph, 0019 and

page 8, paragraph 0072). Therefore it would have been obvious to one having ordinary

skill in the art at the time the invention was made to implement a method of preventing

decryption and viewing of encrypted e-mail message that has expired thought by Udell

into e-mail access restriction system of Anderson, because such method would prevent

a user (recipient) from defeating expiration of messages, further improving security of

the system.

16.   As per claims 2, 3, 8-9, Anderson discloses the electronic mail system (i.e.

system for distributing electronic messages, see figure 1) further comprising a central

electronic mail server (i.e. Message Distribution server (MDS), see figure 1) connected

to the network 140. Anderson discloses the message sender to supply the electronic

message to the MDS and the MDS will stores the message and is responsible for

forwarding it to the recipient [see column 5 lines 1950]. Anderson also discloses the

MDS will retrieve the public key from the recipient and encrypt the electronic message

upon request by the recipient and stream it to corresponding recipient [see figure 6

steps 625,630,635,640]. The recipient can access the message by decrypting it using

the private key of the recipient computer system's private key and display said

electronic message [see column 6 lines 16-29].

17.   As per claims 4-5, Anderson discloses the recipient (i.e. a user) can select a

message and indicate a message forwarding action to be taken (i.e. forward to a

second recipient computer, see figure 2 and column 6 lines 46-65). Anderson discloses

the message distributor subroutine of MDS (i.e. central mail server) being arrange to

encrypt the message using the public encryption key generated in the recipient

computer s, stem [see column 5 lines 58-63] and send it to each Y recipient [column 9

lines 9-16].

18.   As per claim 6, Anderson discloses the central electronic mail server (i.e. MDS)

erases (i.e. deletes) the single copy of the electronic message when the end of a

maximum time period has expired [see column 4 lines 25-44].

19.   As per claim 7, Anderson discloses the central electronic mail server (i.e. MDS)

erases (i.e. deletes) the single copy of the electronic message when the end of a

maximum time period has expired [see column 4 lines 25-44].

20.   As per claims 10-12, Anderson discloses the electronic message (i.e. E-mail) is

encrypted in the central mail server (i.e. Message Distribution Server) with the

recipient's public key before transmission to said recipient computer [see column 10

lines 5-14 and figure 6 steps 625,630,635,640].

21.   As per claims 13, Anderson discloses Message Receiver (MR) stores the

decrypted message indicator (i.e. e-mail) in an encrypted fashion on the recipient

computer system [see column 6 lines 16-29] and erase (i.e. delete) the message if the

expiration period has ended (i.e. upon the occurrence of said date, time, or event, see

column 9 lies 64-66).

22.   As per claims 14-15, Anderson discloses the recipient (i.e. a user) can select a

message and indicate a message forwarding action to be taken (i.e. forward to a

second recipient computer, see figure 2 and column 6 lines 46-65). Anderson discloses

the message distributor subroutine of MDS (i.e. central mail server) being arrange to

encrypt the message using the public encryption key generated in the recipient

computer system [see column 5 lines 58-63] and send it to each recipient [column 9

lines 9-16].

23.   As per claim 16, Anderson discloses the message origination software (i.e.

message sender 154, see figure 1) arranged to permit the message to include the

expiration time (i.e. limitation, see column 3 lines 62-65) before transmission over said

network 140 [see column 3 lines 48-66 and figure 2).

24.   As per claim 17, Anderson does not expressly disclose the processing and

handling limitations are implemented by said view applet (i.e. the message receiver

155). It would have been obvious to a person of ordinary skill in the art at the time of

invention was made to implement the request from the message receiver 155 (i.e. view

applet) of the message recipient to review, save, or delete an indicated message (i.e.

processing and handling limitations) with in the system of Anderson because it's well

known in the art to activate the subroutine software such as view applet in the recipient

computer system to handling the access limitation of the electronic message.

25.   As per claim 34, Anderson discloses an electronic mail system (i.e. system for

distributing electronic messages, see figure 1) comprising

a) a first computer 150 (i.e. the sender, see column 3 lines 61-63) on which is installed message origination software (i.e. message sender software 154, see figure 1) and which is connect to a network 140 capable of carrying an electronic mail message (i.e. transmission of the electronic messages, see column 4 line 65- column 5 line I), said message origination software being arranged to enable an originator of the message to attach message processing limitations to the message before it is sent (i.e. minimum or maximum expiration time is attached to the electronic mail message prior to transmission over network, see column 3 lines 62-67);

b) recipient computers systems (elements 160, 170, and 180; see figure 1) are connected to network 140 [see column 4 lines 59-65],

c) a viewer applet (i.e. the message receiver 155 with the URL, the web browser software, see column 4 lines 13-16);

d) a central electronic mail server (i.e. Message Distribution server (MDS), see figure 1) connected to the network 140. Anderson discloses the message sender to supply the electronic message to the MDS and the MDS will stores the message and is responsible for forwarding it to the recipient [see column 5 lines 19-50]. Anderson also discloses the MDS will retrieve the public key from the recipient and encrypt the electronic message upon request by the recipient and stream it to corresponding recipient [see figure 6 steps 625,630,635,40]. The recipient can access the message by decrypting it using the private key of the recipient computer system's private key and display said electronic message [see column 6 lines 16-29].

Anderson also discloses the processing limitations (i.e. restriction on access by some or all recipients, see column 3 line 65-column 4 line 1) are implemented by said central electronic mail server (i.e. MDS) and message receiver 155 (i.e. said view applet, see figure 1). Anderson does not explicitly teach preventing decryption and viewing of encrypted messages by a recipient unless processing limitations are implemented.

However, Udell teaches a viewer applet (i.e. application program (Microsoft outlook), see page 6, paragraph 0064) is arranged to prevent decryption and viewing of encrypted electronic mail message by a recipient unless processing limitations are implemented (i.e. message expirations are valid, see page 2, paragraph, 0019 and page 8, paragraph 0072). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement a method of preventing decryption and viewing of encrypted e-mail message that has expired thought by Udell into e-mail access restriction system of Anderson, because such method would prevent a user (recipient) from defeating expiration of messages, further improving security of the system.

26. As per claim 35, Anderson discloses the message is encrypted by MDS using a public key generated by the message receiver 155 (i.e. said view applet, see figure 1) and decrypted with corresponding private key in the recipient computer system [see figure 6 steps 625-640 and figure 7 step 715].

27.   As per claims 36-37, Anderson discloses the recipient (i.e. a user) can select a
message and indicate a message forwarding action to be taken (i.e. forward to a
second recipient computer, see figure 2 and column 6 lines 46-65). Anderson discloses
the message distributor subroutine of MDS (i.e. central mail server) being arrange to
encrypt the message using the public encryption key generated in the recipient
computer system [see column 5 lines 58-631 and send it to each recipient [column 9
lines 9-16].

28.   As per claims 38-40, the claimed steps correspond to the functions of the
elements of the apparatus claims 34-37, which has been rejected above and thus
rejected with the same reason applied thereto.

29.   As per claim 41, Anderson discloses a computer program for handling electronic
mail comprising: a) a mail original portion (i.e. message sender 154, see figure 1)
arranged to permit the sender to supply messaging sending information including
optional information as minimum and maximum expiration time (i.e. a date, time or
event, see column 3 lines 62-65). The Message Receiver (MR) stores the decrypted
message indicator (i.e. e-mail) in an encrypted fashion on the recipient computer
system [see column 6 lines 16-29] and erase (i.e. delete) the message if the expiration
period has ended (Le. upon the occurrence of said date, time, or event, see column 9
lies 64-66). b) a view applet portion (i.e. message receiver 155, see figure 1) arranged
to access the message by decrypting it using the private key of the recipient computer

system's private key and display said electronic message [see column 6 lines 16-29]

and. permit viewing of the received electronic message before the expiration time period

end [see column 9 lines 66-67].

Anderson does not explicitly teach preventing decryption and viewing of

encrypted messages by a recipient after the occurrence of date, time or event selected

by the originator of the message.

However, Udell teaches a viewer applet (i.e. application program (Microsoft

outlook), see page 6, paragraph 0064) is arranged to prevent decryption and viewing of

encrypted electronic mail message by a recipient after the occurrence of the date, time

or event by said originator of the electronic mail message (page 2, paragraph, 0019 and

page 8, paragraph 0072). Therefore it would have been obvious to one having ordinary

skill in the art at the time the invention was made to implement a method of preventing

decryption and viewing of encrypted e-mail message that has expired thought by Udell

into e-mail access restriction system of Anderson, because such method would prevent

a user (recipient) from defeating expiration of messages, further improving security of

30.   As per claim 42, Anderson discloses a computer program of the MDS will retrieve

the public key from the recipient and encrypt the electronic message upon request by

the recipient and stream it to corresponding recipient [see figure 6 steps

625,630,635,640]. The recipient can access the message by decrypting it using the

private key of the recipient computer system's private key and display said electronic

message [see column 6 lines 16-29].

31.	As per claim 43, Anderson discloses the compute program to erase (i.e. delete) the message if the expiration period has ended (i.e. upon the occurrence of said date, time, or event, see column 9 lies 64-66).

32.	As per claims 44-45, Anderson discloses the mail original portion (i.e. message sender 154, see figure 1) arranged to permit the sender to attach a copy of said view applet portion (i.e. message receiver 155, see figure 1) to each message including optional information as minimum and maximum expiration time (i.e. a specified expiration date, time or event, see column 3 lines 6265). Anderson also discloses the message tracking table is arranged to implement handling and processing controls on a received message [see figure 2].

33.	As per claims 46-50, the claimed steps Correspond to the functions of the elements of the apparatus claims 41-45, which has been rejected above, and thus rejected with the same reason applied thereto.

Response to Arguments

34.	Applicant's arguments with respect to claims 1-17 and 34-50 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

35.   Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W Dada whose telephone number is (703) 305-8895. The examiner can normally be reached on Monday - Friday (8:30 am - 6:00 pm).
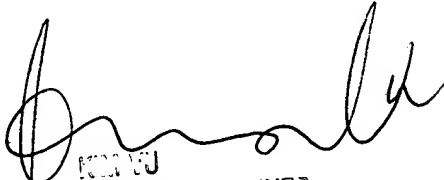
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada

February 18, 2004